UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/519,068	10/31/2005	Antonius H.M. Akkermans	NL 020645	7468

24737 7590 08/20/2009
PHILIPS INTELLECTUAL PROPERTY & STANDARDS
P.O. BOX 3001
BRIARCLIFF MANOR, NY 10510

EXAMINER	
CHAI, LONGBIT	

ART UNIT	PAPER NUMBER
2431	

MAIL DATE	DELIVERY MODE
08/20/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/519,068	AKKERMANS ET AL.	
	Examiner	Art Unit	
	LONGBIT CHAI	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03 June 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3-5,7-11,13,15 and 16* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *3 and 7* is/are allowed.

6)☒ Claim(s) *1,4,5,8-11,13,15 and 16* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *22 December 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Currently pending claims are 1, 3 – 5, 7 – 11, 13, 15 and 16.

Response to Arguments

2. Applicant's arguments with respect to the subject matter of the instant claims have been fully considered but are not persuasive.

3. As per claim 1, Applicant assets Kulinets does not teach "the record carrier is designed such that the first (HCK) and the second (UCID) parts of decryption information can not be read from the record carrier" because "Kulinets discloses regarding transponder 2, the stored information necessary for calculating the decryption key FDK may not be read from transponder 2" (emphasis added, col. 3, lines 48-44). Therefore, the decryption information is not readable from the record carrier of Kulinets" (Remarks: Page 6 Last Para). Examiner respectfully disagrees with the following rationale:

- (a) Kulinets teaches the transponder 2 transmits the decryption key FDK via the bi-directional link 17 to the transceiver 25. The frame decryption key FDK is used in a decryption circuit 19 to decrypt the encrypted frame data which follows the frame header (Kulinets: Column 3 Line 39 – 44 and Column 4 Line 21 – 26). A transceiver 25 communicates with the transponder 2 through an electromagnetic bi-directional link 17. As the distances are small, the required transmission channel power is very low. Further, the reader 20 and its associated transceiver 25 generate a magnetic field which is used to transmit operational power to the transponder 2 (Kulinets: Column 3 Line 19 – 24).
- (b) Therefore, Kulinets indicates it will be evident when describing the details of transponder 2, the stored information necessary for calculating the decryption key FDK may

not be *read* from the transponder 2 – (i.e. in the case w/o the specially designed electromagnetic bi-directional link 17 as presented above in (a) and besides, Examiner notes if the information would never be able to get read out from the non-volatile memory for use, then what is for to store said information in memory in the first place) and thus, Kulinets discloses while it may be possible to reproduce the stored data 1, without a corresponding transponder 2 having the secret information embedded therein for deriving a decryption key FDK, the duplicated ODC 1 is useless (Kulinets: Column 3 Line 50 – 55). Accordingly, **Examiner notes** *Applicant's argument has no merit since the alleged limitation (i.e. exactly how to read the data from the record carrier) has not been recited into the claim. Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See In re Van Geuns, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).*

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraph of 35 U.S.C. 102 that forms the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

4. Claims 1, 4, 5, 8 – 11, 13, 15 and 16 are rejected under 35 U.S.C. 102(b) as being anticipated by Kulinets U.S. Patent 6,005,940).

As per claim 1, 9 and 13, Kulinets teaches a record carrier (Kulinets: Figure 2) having:

a first area storing information (data), which is at least partly stored in encrypted form (E_{AK}(data)), this part being called an asset (E_{AK}(data)) (Kulinets: Column 2 Line 10 – 12: a main data field where the scrambled data (i.e. (E_{AK}(data)) is recorded, as taught by Kulinets, is considered as a first area), and which includes a first part of decryption information (HCK, E_{DNK}(HCK)) (Kulinets: Column 5 Line 51 – 54 and Column 56 – 59: for one of examples, the frame serial number is an input to the deciphering engine to decrypt the encrypted data, which can be considered a part of the "decryption information"), and the record carrier further having,

a second area storing a second part of decryption information (UCID) (Kulinets: Column 6 Line 36 – 41: the DK_A and its derived key FEK_i for each frame number i are stored in the transponder, which can be considered a part of the "decryption information"); and

both the first (HCK) and second (UCID) parts of decryption information serve in decrypting the asset (E_{AK}(data)) (Kulinets: Column 6 Line 36 – 67);

wherein the first area comprises a storage medium of one physical kind and the second area comprise a storage medium of another physical kind (Kulinets: Column 3 Line 1 – 6 / Line 49 – 55: a transponder, fixed to the disk medium, contains a microelectronic chip having secret information embedded therein for deriving a decryption key to decrypt the data content can be considered as a separate storage medium of another physical kind), and

wherein the record carrier is designed such that the first (HCK) and the second (UCID) parts of decryption information can not be read from the record carrier (Kulinets: Column 4 Line 21 – 26, Column 4 Line 5 – 8 and Column 3 Line 64 – 65, Column 3 Line 39 – 44 and Column 3 Line 50 – 55: (a) the transponder 2 transmits the decryption key FDK via the bi-directional link 17 to the transceiver 25. The frame decryption key FDK is used in a decryption circuit 19 to decrypt the encrypted frame data which follows the frame header (Kulinets: Column

3 Line 39 – 44 and Column 4 Line 21 – 26). A transceiver 25 communicates with the transponder 2 through an electromagnetic bi-directional link 17. As the distances are small, the required transmission channel power is very low. Further, the reader 20 and its associated transceiver 25 generate a magnetic field which is used to transmit operational power to the transponder 2 (Kulinets: Column 3 Line 19 – 24)).

As per claim 4, Kulinets teaches a symmetric method using a first cryptographic key, called an asset key (AK), is used for asset encryption and decryption, and in that the asset key (AK) is stored in the second area in an encrypted form, wherein for its encryption a symmetric encryption method has been used (Kulinets: Column 2 Line 20 – 24, Column 6 Line 38 – 41 and Column 1 Line 65 – 67: a decryption key, as an asset key, is obtained at the transponder and is used to decrypt the encrypted data), this method employing a second cryptographic key (CIDK) in whose derivation both the first (HCK) and second (UCID) parts of decryption information have been used (Kulinets: Column 6 Line 59, Column 7 Line 14 – 16, Column 6 Line 13 – 15 and Column 8 Line 26 – 27: (a) the medium data track is divided into frames of encrypted data (b) a deciphering key DK_A along with the frame identification number can be combined to generate another decryption key).

As per claim 5, Kulinets teaches a third cryptographic key, called a hidden-channel key (HCK), serves in the asset decryption (Kulinets: Column 2 Line 20 – 24: a decryption key that can be derived at the transponder, which is used to decrypt the encrypted data, can also be considered as a hidden-channel key), and in that the hidden-channel key (HCK) is obtainable from the first part of decryption information (HCK, E_{DNK}(HCK)), in particular, that the hidden-channel key (HCK) coincides with the first part of decryption information (HCK) and that the first part of decryption information (HCK) is scrambled and/or encrypted within the information (data)

stored in the first area (Kulinets: Column 6 Line 36 – 41: each of the hidden-channel keys FEK_i, as a data decryption key, can be obtained from DK_A and each frame number i – i.e. coincides with the first part of decryption information).

As per claim 7, Kulinets teaches the chip is designed for checking the right of an reading and/or writing device to access the record carrier (Kulinets: Column 3 Line 1 – 6, Column 2 Line 25 – 30. Column 7 Line 50 – 59 and Column 8 Line 25 – 28: the chip embedded within the transponder uses a challenge / response protocol to authorize the access to content data where a frame identification number is used as a part of the challenge value).

As per claim 8, Kulinets teaches the second area is designed for storing user-specific settings serving in controlling the access of an reading and/or writing device to the record carrier and/or in controlling the manner information being read from the record carrier is presented by the reading and/or writing device to a user of the reading and/or writing device (Kulinets: Column 3 Line 58 – 62: the stored DK_A which is unique for any particular ODC title, can be considered as an user-specific settings).

As per claim 10, Kulinets teaches the device is designed for accessing the first and second areas of the record carrier in parallel (Kulinets: Column 3 Line 1 – 6 / Line 52 – 55: a transponder, fixed to the disk medium, contains a separate hardware device (i.e. a microelectronic chip) having its own processor and memory so that the first and second areas of the record carrier can be accessed in parallel).

As per claim 11, Kulinets teaches the device is designed for storing and maintaining a revocation list of identifiers (UCID), and for at least partly refusing a user of the device access to a record carrier if the identifier (UCID) being stored on the record carrier belongs to the

revocation list (Kulinets: Column 6 Line 6 – 12 and Colum 6 Line 36 – 43: (a) the use of region code identification information is compared with reproduction permission information to authorize the reproduction of content data on a particular permitted region and as such the region code identification information that has the mismatch with he reproduction permission information on a particular permitted region is considered as falling in a part of the revocation list of identifiers and (b) For each compilation of data to be stored on a data medium, a separate secret deciphering key DK_A is selected and this value of DK_A will be written in the non-volatile memory of the transponder of the ODC having this particular encrypted data and used by the transponder to derive a key to decrypt a stored data).

As per claim 15, Kulinets teaches the device is further designed for obtaining complete decryption information from both the first (HCK, EDNK(HCK)) and second parts (UCID) of decryption information, and for decrypting and/or encrypting the asset (EAK(data)) with the complete decryption information (Kulinets: Column 4 Line 23 – 29 and Column 6 Line 13 – 15).

As per claim 16, Kulinets teaches obtaining complete decryption information from both the first (HCK, EDNK(HCK)) and second parts (UCID) of decryption information, and decrypting and/or encrypting the asset (EAK(data)) with the complete decryption information (Kulinets: Column 4 Line 23 – 29 and Column 6 Line 13 – 15).

Allowable Subject Matter

5. Claims 3 and 7 are allowed.

The following is an examiner's statement of reasons for allowance: The present invention is directed to a device (a record carrier) for decrypting the encrypted payload data with a first area and a second area, which comprises a chip to store a first counter (C_i) and the second counter (C_e); wherein the second counter (C_e) is stored in an encrypted form and the first (HCK) and second (UCID) parts of decryption information serve in decrypting the second counter (C_e). Both of the closest prior art, U.S. Pattern 6,289,102 and U.S. Pattern 6,005,940, fails to anticipate or render obvious the claimed invention.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LONGBIT CHAI whose telephone number is (571)272-3788. The examiner can normally be reached on Monday-Friday 9:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William R. Korzuch can be reached on 571-272-7589. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Longbit Chai/

Longbit Chai E.E. Ph.D
Primary Examiner, Art Unit 2431
8/16/2009